1. In a client computing system, a method for receiving credentials that can be used to can authentic with a server computing system, the method comprising:

an act of receiving a limited-use credential;

an act of establishing a secure link between the client computing system and the server computing system;

an act of submitting the limited-use credential to the server computing system over the established secure link; and

an act of receiving an additional credential that can be used for subsequent authentication with the server computing system, the additional credentials being provisioned at the sever computing system based on the limited-use credential.

2. The method as recited in claim 1, wherein the limited-use credential is a single-use password.

3. The method as recited in claim 1, wherein establishing a secure link between the client computing system and the server computing system comprises generating a session key based on Diffie-Hellman public keys of the client computing system and the server computing system.

4. The method as recite in claim 1, wherein the an act of receiving an additional credential that can be used for subsequent authentication with the server computing system comprises an act of receiving a certificate that can be used to access a wireless network.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

5. In a server computing system, a method for providing credentials to a client computing system, the method comprising:

an act of establishing a secure link between the server computing system and the client computing system;

an act of receiving a limited-use credential from the client computing system over the established secure link, the limited-use credential authenticating the client computing system;

an act of provisioning an additional credential for the client computing system based on the received limited-user credential, the additional credential for subsequently authenticating the client computing system; and

an act of sending the additional credential to the client computing system over the established secure link.

6. The method as recited in claim 5, wherein establishing a secure link between the server computing system and the client computing system comprises generating a session key based on Diffie-Hellman public keys of the server computing system and the client computing system.

7. The method as recited in claim 5, wherein the limited-use credential is a single-use password.

8. The method as recited in claim 5, wherein the act of provisioning an additional credential for the client computing system based on the received limited-user credential comprises provisioning a certificate that can be used to access a wireless network.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

9. In a client computing system, a method for participating in authentication with a server computing system, the method comprising:

an act of receiving a first server request that includes at least the authentication mechanisms deployed at the server computing system;

an act of sending a first response that includes at least the authentication mechanisms deployed at the client computing system;

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and server computing system;

an act of receiving a second server request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key;

an act of decrypting the encrypted authentication content with the tunnel key to reveal unencrypted authentication content, the unencrypted authentication content indicating a mutually deployed authentication mechanism; and

an act of sending a second response, the second response including encrypted response data that is responsive to the unencrypted authentication content, the encrypted response data for authenticating with the server computing system according to the mutually deployed authentication mechanism.

10. The method as recited in claim 9, wherein the first server request includes the authentication mechanisms deployed at the server computing system, a previous packet ID and a Nonce.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

11. The method as recited in claim 9, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

12. The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

13. The method as recited in claim 9, wherein the first response includes the authentication mechanisms deployed at the client computing system, a previous packet ID, a nonce, one or more security associations, and one or more public keys.

14. The method as recited in claim 9, wherein the act of identifying a tunnel key comprises deriving a tunnel key based on a shared secret, a client side nonce, and a server side nonce.

15. The method as recited in claim 9, wherein the act of receiving a second server request comprises receiving encrypted authentication content corresponding to an authentication method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot-

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

16. The method as recited in claim 9, wherein the second server request includes encrypted authentication content, a previous packet ID, a security association, and a public key.

17. The method as recited in claim 9, wherein the act of sending a second response includes sending encrypted responsive data for an authentication method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

18. The method as recite in claim 9, wherein the second response includes encrypted responsive data and a previous packet ID.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

19. In a server computing system, a method for participating in authentication with a client computing system, the method comprising:

an act of sending a first request that includes at least the authentication mechanisms deployed at the server computing system;

an act of receiving a first client response that includes at least the authentication mechanisms deployed at the client computing system;

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and server computing system;

an act of sending a second request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key, the encrypted authentication content indicating a mutually deployed authentication mechanism; and

an act of receiving a second client response, the second client response including encrypted response data that is responsive to the encrypted authentication content, the encrypted response data for authenticating with the server computing system according to the mutually deployed authentication mechanism.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

20. The method as recited in claim 19, wherein the first request includes the authentication mechanisms deployed at the server computing system, a previous packet ID and a Nonce.

21. The method as recited in claim 19, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic

Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

22. The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

23. The method as recited in claim 19, wherein the first client response includes the authentication mechanisms deployed at the client computing system, a previous packet ID, a nonce, one or more security associations, and one or more public keys.

24. The method as recited in claim 19, wherein the act of identifying a tunnel key comprises deriving a tunnel key based on a shared secret, a client side nonce, and a server side nonce.

25. The method as recited in claim 19, wherein the act of sending a second request comprises sending encrypted authentication content corresponding to an authentication method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

26. The method as recited in claim 19, wherein the second request includes encrypted authentication content, a previous packet ID, a security association, and a public key.

27. The method as recited in claim 19, wherein the act of receiving a second client response includes receiving encrypted responsive data for an authentication method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

28. The method as recite in claim 19, wherein the second client response includes encrypted responsive data and a previous packet ID.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111